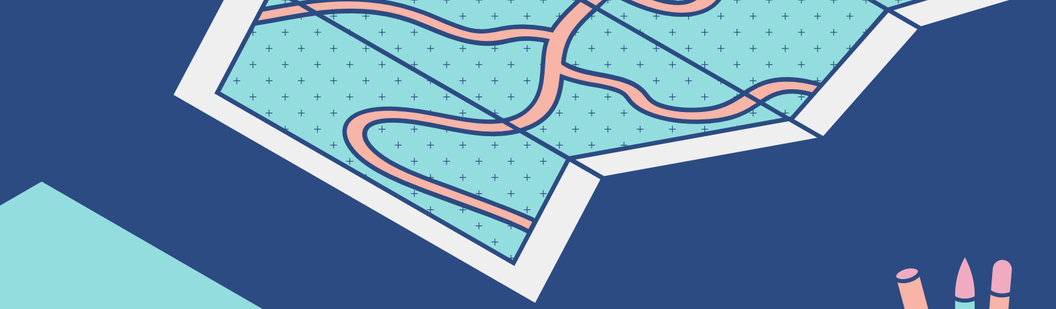
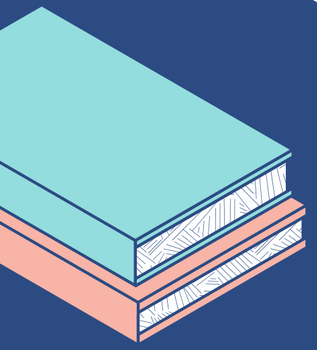
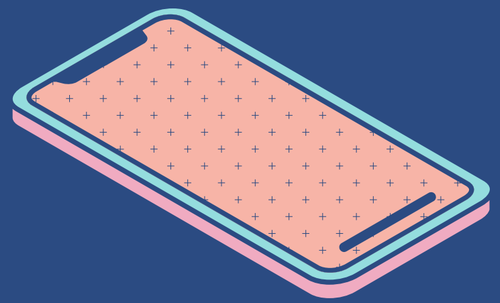
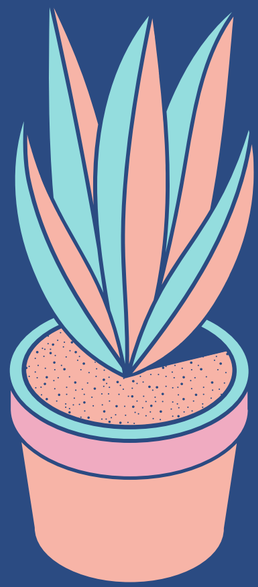
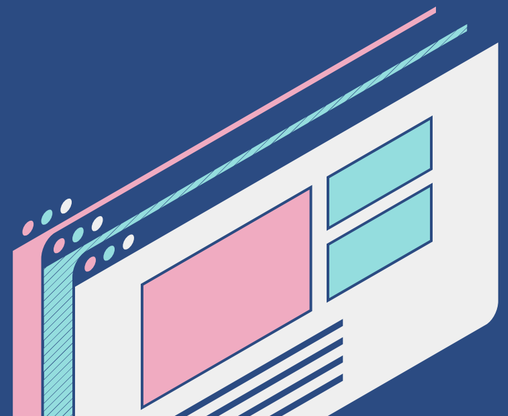
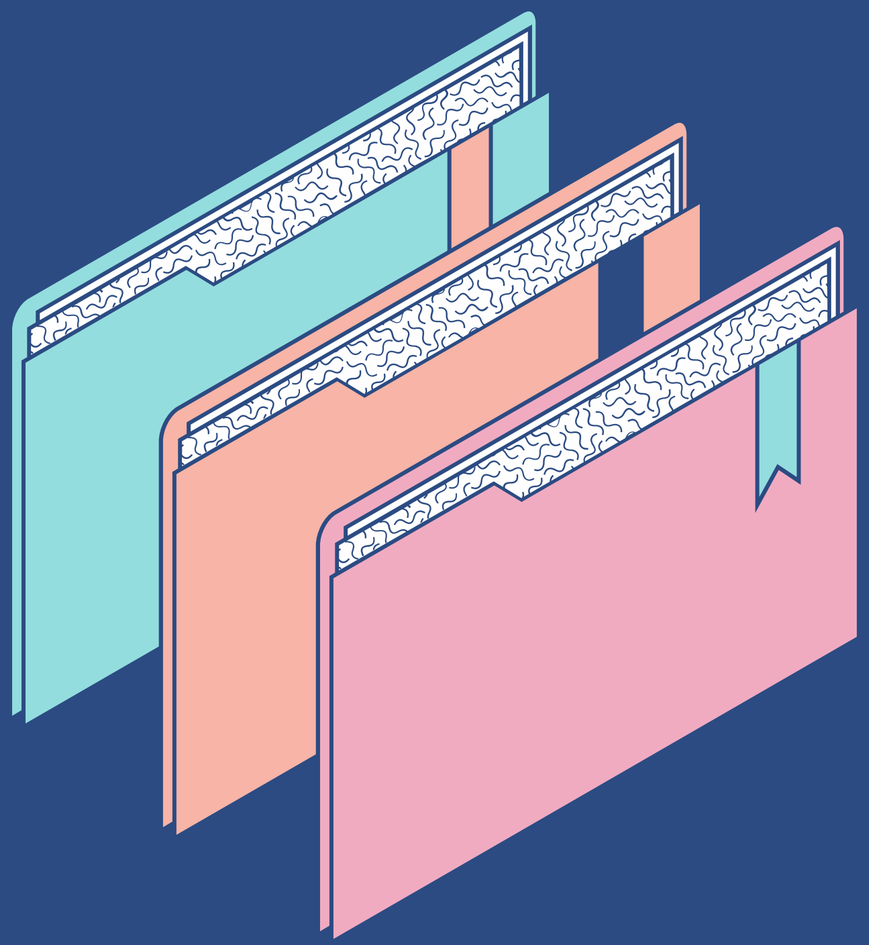



ТЕМА ДОКЛАДА:

Биометрия в мобильных устройствах

Выполнили: Кутьин Захар
Крутов Алексей

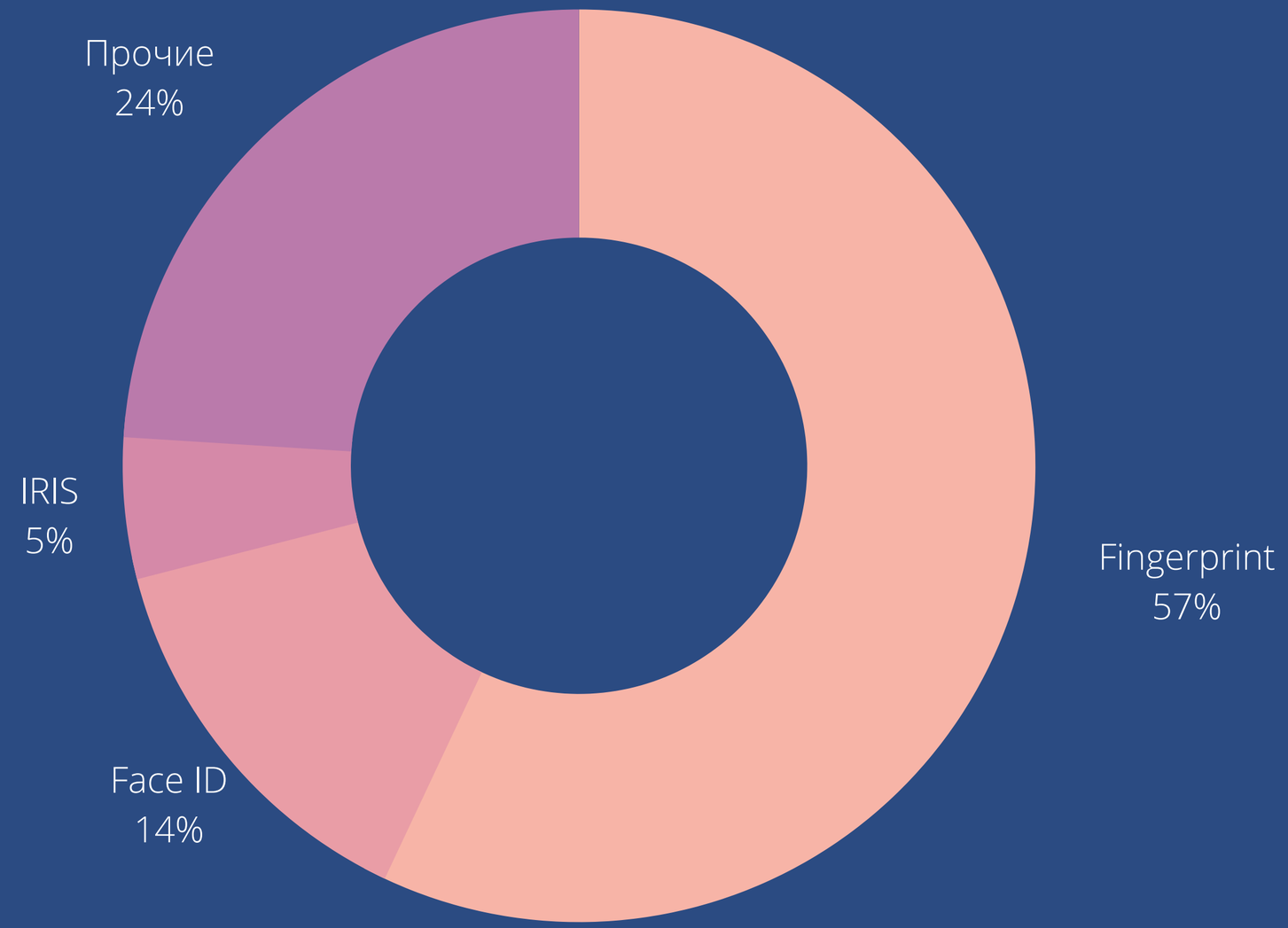


Введение

- Широкое использование и возможности мобильных технологий сформировали потребность людей вести свою личную и деловую жизнь в движении. Для удовлетворения данной потребности мобильная связь, приложения, установленные на мобильные устройства, и транзакции должны быть защищены для обеспечения конфиденциальности пользователя и целостности транзакций. Это необходимо для создания доверенной среды мобильных платформ, в которой могут участвовать как отдельные лица, так и предприятия, некоммерческие организации и правительства. Аутентификация пользователя, удостоверяющая его личность, является важной частью создания этой среды.

Основные виды биометрии в мобильных устройствах

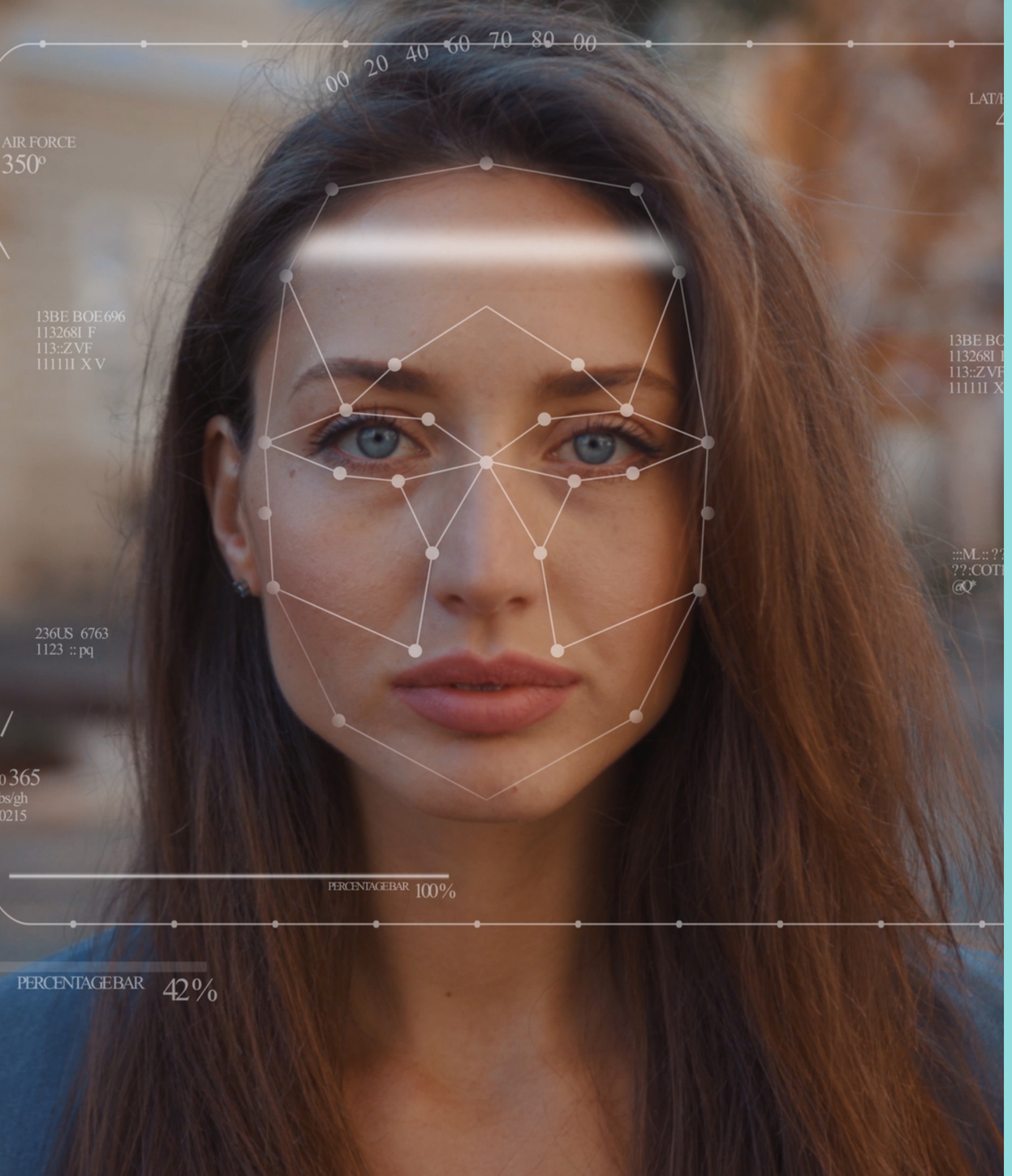
- Сканер отпечатка пальца (fingerprint) – 57%
- Сканер геометрии лица (face ID) – 14%
- Сканеры радужной оболочки глаза (IRIS) и геометрии руки – 3-5%
- Прочие: голосовая биометрия и др. – 24%



Сканер отпечатка пальца (fingerprint)

Для того, чтобы «узнать» пользователя по отпечатку пальца и безопасно хранить его данные, каждый производитель мобильных устройств предлагает свои возможности. Так, на устройствах Apple образец отпечатка пальца проводится через хеш-функцию перед сохранением в защищенный вычислительном модуль. На устройствах Android степень безопасности зависит от производителя, используемых им подходов и решений.
Недостатки:

- Не надежные сенсоры
- Высокий риск взлома.
- Возможны проблемы с аутентификацией.



Сканер геометрии лица (face ID)

Если приложение идентифицирует пользователя по лицу, сканирование осуществляют за счет емкостной камеры.
Здесь требуется еще более сложный алгоритм, требующий высокой точности захвата изображения и распределения более 30 тысяч контрольных точек по изображению лица пользователя. В свою очередь, это определяет более высокие требования к камере смартфона.

Недостатки:

- Не все устройства имеют Face ID
- Риск сканирования фотографии владельца
- 3D печать лица

Сканер радужной оболочки глаза (IRIS)

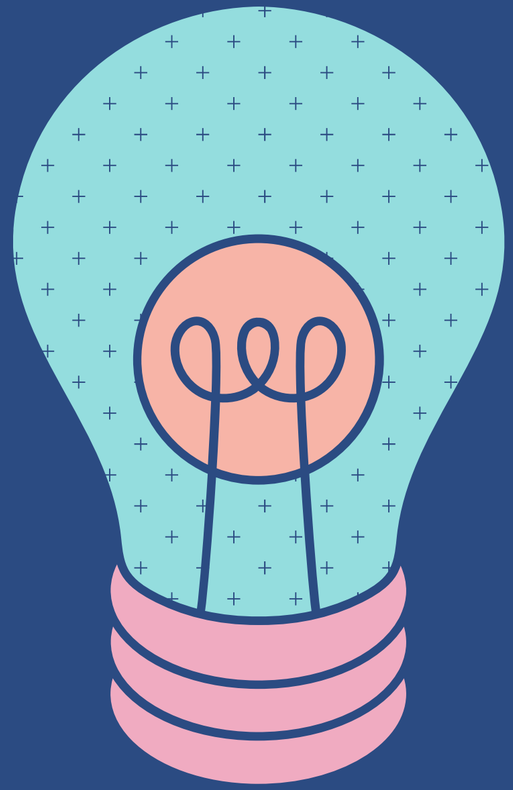
Важно помнить, что IRIS – это не сканер сетчатки глаза. Проще говоря, эта технология сканирует радужную оболочку, которая окружает зрачок, тогда как сетчатка располагается внутри глаза на задней стенке. Сканер определяет те или иные особенности внешности пользователя и геометрическую форму радужки, используя емкостные камеры
Недостатки:

- Риск взлома при одновременном использовании фотографии и контактных линз.

Международные стандарты:

- ПНСТ 379—2019 Информационные технологии. Биометрия. Применение биометрии в мобильных устройствах
- ISO/IEC TR 30125:2016, Information technology — Biometrics used with mobile devices, MOD)

Биометрия позволяет снизить необходимость в запоминании и постоянном вводе сложного пароля, что будет по душе и пользователям и администраторам. Но не стоит забывать, что идеальной защитной системы не существует. Поэтому советуем использовать несколько способов защиты информации, менять пароли хотя бы раз в полгода\год и придумать все более сложные способы защиты.



Спасибо за внимание

Мы надеемся, что вы узнали что-то новое.